California Public Employees' Retirement System

Attachment 1

Information Security Office
Information Security Internal Incident Tracking Log

Official (Via E-Mail) Notification Date of Incident Sent to ISOF	Originating Division or Office	Working Title	Type of Incident	Comments
6/7/2010	CDOP Management	Unauthorized Entry without Guest Badge Access Card	EDD Delivery Person Entering LPN 5th Floor	Colliers International reviewed the cameras and determined that the EDD Delivery Person entered the building (LPN) through the 1st floor mantrap on the P Street side. The delivery person went to the directory and went straight to the elevator up to 5th floor. He did not stop to ask security any questions. He got off on the 5th floor and tried to enter the double glass door but could not enter. Someone from the inside walked by and motioned his hand to activate the REX (the sensor on the office side that unlocks the doors to allow someone to exit into the elevator vestibule) to unlock the door and that is how the delivery person gained access into the work area. Colliers International could not identify the person who activated the REX. Unfortunately, this is an example of a staff person trying to be helpful. The intent of the new "Support Safety. Build Security." Campaign is to educate building occupants regarding these situations.
6/11/2010	ISOF	Personal Use of State Resources	Violation of 8314 Government Code and CalPERS policy	A security analyst in the Information Security Office, reviewed a Websense report on June 11, 2010 and noticed a significant number of hits (ove 700,000) to one web site. The user PC was in ITSB. The PC was disconnected from the CalPERS network and examined. On the basis of that examination it was concluded that the ITSB employee was developing and operating a personal web site using state time and state resources. The employee resigned state service.
6/28/2010	SMSD Employee	City of Carlsbad Deduction Register	Possible Disclosure of Member's Information	The City of Carlsbad deduction register was mailed Fed Ex to the City of Carlsbad. It appears that the Fed Ex envelope was rejected/returned by the City of Carlsbad and sent back to CalPERS. It appears that the CalPERS mailroom must have mistakenly sorted and routed it to SMSD. The BNSD has contacted the mailroom to bring this to their attention. The BNSD contacted the City of Carlsbad to determine why the deduction register was returned. The City of Carlsbad determined that the Deduction Register was refused because the person CalPERS had as the "attention" person had not been at City Hall in the past 10 years. The City of Carlsbad had apparently not contacted CalPERS previously to have the contact information corrected. CalPERS will update the CalPERS records with the administration office address to prevent this mailing address error from happening in the future. No member information was exposed.
7/9/2010	ISOF	Potential Malicious Site Activity	Potential System Infection	A security analyst in the Information Security Office, reviewed a Websense report on Friday, July 9, 2010 and noticed a significant amount of hits to a specific "malicious site" starting at midnight. The user PC was in INVO. The analyst conducted an initial research of the URL and detected several references to "Zeus" which is a widely known Trojan horse malware that steals information by keystroke logging. Zeus is spread mainly through drive-by downloads and phishing schemes . No CalPERS data was disclosed as Websense blocked all attempts by the PC to access the malicious website. The PC was disconnected from the CalPERS network on 7/9/10 at approximately 1:30 PM. It is likely that the malicous program was installed because the employee had local administrator rights to his PC. The PC was reimaged and redeployed to the employee without local administrator rights.

Attachment 1

California Public Employees' Retirement System

Information Security Office
Information Security Internal Incident Tracking Log

Official (Via E-Mail) Notification Date of Incident Sent to ISOF	Originating Division or Office	Working Title	Type of Incident	Comments
7/19/2010	ITSB	Unauthorized Disclosure of Social Security Numbers on CalPERS FTP Server	Unauthorized Disclosure of SSN	The Association Group Insurance Administrators (AGIA) is an external partner that creates, markets, and administers Insurance Programs for its clients (e.g., CalPERS)> AGIA uses a middleware "file relay" ftp service to retrieve and upload encrypted files for the carrier deduction process. The files are encrypted and decrypted using PGP/GPG compliant encryption software. On July 8, 2010 AGIA uploaded an unencrypted file to the CalPERS secure server. This unencrypted file contained 210 Social Security numbers without names. The file remained on the external ftp server until July 19, 2010. At that time a software specialist from the middleware applications in ITSB found the problem and had it corrected. The file was removed from the secure server. The California Law on Notice of Security Breach does not apply because the file did not contain in combination with the first names or initials and last names of those persons whose Social Security numbers were not encrypted on the file. In addition, the information was not accessed or downloaded while on the secure server. AGIA staff were reminded of the requirement to comply with the CalPERS Electronic File Transfers to External Parties Practices and Procedure.